AMENDMENTS TO THE CLAIMS

1 - 6. (Cancelled)

7. (Currently Amended) The outsource source encryption device of Claim 35[[6]], wherein

the certification information is generated based on identity information of the outsource source encryption device.

8. (Original) The outsource source encryption device of Claim 7, wherein

the certification information is a certifier generated using secret key encryption, and

the individual information is a secret key used in the secret key encryption .

9. (Original) The outsource source encryption device of Claim 7, wherein

the certification information is digital signature data generated using public key encryption, and

the individual information is a secret key of the public key encryption.

10. (Currently Amended) The outsource source encryption device of Claim 32[[1]], wherein

the receiving unit further receives fourth license information that includes third license information proving that another encryption device has permission to use the content from a content distribution device and proves that the other encryption device has outsourced the encryption of the content to the outsource source encryption device,

the generating unit generates fifth license information that includes the fourth license information and proves that encryption has been outsourced to the outsource destination encryption device, and

the transmission unit transmits the fifth license information together with the content to the outsource destination encryption device.

11 - 20. (Cancelled)

21. (Currently Amended) An integrated circuit used in an outsource source encryption device that has permission to encrypt content received from a content distribution device, and

outsources encryption of the received content to an outsource destination encryption device, the integrated circuit comprising:

a receiving unit operable to receive first license information proving that the outsource source encryption device has permission from the content distribution device to use the content;

a generating unit operable to (i) generate certification information based on the first license information using identification information of the outsource source encryption device, and (ii) generate second license information that proves that encryption of the content has been outsourced to the outsource destination device, the second license information including the first license information and the certification information; and ~~includes the received first license information and proves that encryption of the content has been outsourced to the outsource destination encryption device; and~~

a transmission unit operable to transmit the generated second license information together with the received content to the outsource destination encryption device.

22. (Cancelled)

23. (Currently Amended) An outsourcing method used in an outsource source encryption device that has permission to encrypt content received from a content distribution device, and outsources encryption of the received content to an outsource destination encryption device, the outsourcing method comprising steps of:

a receiving step of a receiving unit receiving first license information proving that the outsource source encryption device has permission from the content distribution device to use the content;

a generating step of a generating unit (i) generating certification information based on the first license information using identification information of the outsource source encryption device, and (ii) generating second license information that proves that encryption of the content has been outsourced to the outsource destination encryption device, the second license information including the first license information and the certification information; and ~~that includes the received first license information and proves that encryption of the content has been outsourced to the outsource destination encryption device; and~~

a transmission step of a transmission unit transmitting the generated second license

information together with the received content to the outsource destination device.

24. (Cancelled)

25. (Currently Amended) A non-transitory computer readable recording medium on which is recorded an outsourcing program used in an outsource source encryption device that has permission to encrypt content received from a content distribution device, and outsources encryption of the received content to an outsource destination encryption device, wherein when executed the outsourcing program causes a computer to perform a method comprising:

a receiving step of a receiving unit receiving first license information proving that the outsource source encryption device has permission from the content distribution device to use the content;

a generating step of a generating unit generating (i) certification information based on the first license information using identification information of the outsource source encryption device, and (ii) second license information that proves that encryption of the content has been outsourced to the outsource destination encryption device, the second license information including the first license information and the certification information; and ~~that includes the received first license information and proves that encryption of the content has been outsourced to the outsource destination encryption device; and~~

a transmission step of a transmission unit transmitting the generated second license information together with the received content to the outsource destination device.

26 - 31. (Cancelled)

32. (New) An outsource encryption device that has permission to encrypt content received from a content distribution device, and outsources encryption of the received content to an outsource destination encryption device, the outsource source encryption device comprising:

a receiving unit operable to receive first license information proving that the outsource source encryption device has permission from the content distribution device to use the content;

a generating unit operable to (i) generate certification information based on the first license information using identification information of the outsource source encryption device,

and (ii) generate second license information that proves that encryption of the content has been outsourced to the outsource destination encryption device, the second license information including the first license information and the certification information; and

a transmission unit operable to transmit the generated second license information together with the received content to the outsource destination encryption device.

33. (New) An outsource encryption device that has permission to encrypt content received from a content distribution device, and outsources encryption of the received content to an outsource destination encryption device, the outsource source encryption device comprising:

a receiving unit operable to receive first license information proving that the outsource source encryption device has permission from the content distribution device to use the content;

a generating unit operable to (i) generate certification information based on the first license information using a secret key used in secret key encryption in the outsource source encryption device, the certification information being a certifier generated using the secret key information, and (ii) generate second license information that proves that encryption of the content has been outsourced to the outsource destination encryption device, the second license information including the first license information and the certification information; and

a transmission unit operable to transmit the generated second license information together with the received content to the outsource destination encryption device.

34. (New) An outsource encryption device that has permission to encrypt content received from a content distribution device, and outsources encryption of the received content to an outsource destination encryption device, the outsource source encryption device comprising:

a receiving unit operable to receive first license information proving that the outsource source encryption device has permission from the content distribution device to use the content;

a generating unit operable to (i) generate certification information based on the first license information using a secret key used in public key encryption in the outsource source encryption device, the certification information being digital signature data generated using the public key encryption, and (ii) generate second license information that proves that encryption of the content has been outsourced to the outsource destination encryption device, the second license information including the first license information and the certification information; and

a transmission unit operable to transmit the generated second license information together with the received content to the outsource destination encryption device.

35. (New) An outsource encryption device that has permission to encrypt content received from a content distribution device, and outsources encryption of the received content to an outsource destination encryption device, the outsource source encryption device comprising:

a receiving unit operable to receive first license information proving that the outsource source encryption device has permission from the content distribution device to use the content, the first license information including certification information generated using individual information particular to the content distribution device;

a generating unit operable to generate second license information that includes the received first license information and proves that encryption of the content has been outsourced to the outsource destination encryption device;

a transmission unit operable to transmit the generated second license information together with the received content to the outsource destination encryption device.